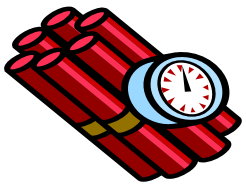
START HERE GO FURTHER FEDERAL STUDENT AID

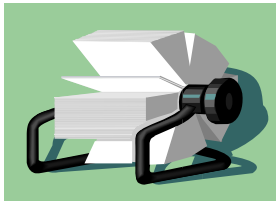
FINANCIAL MANAGEMENT SYSTEM




Federal Student Aid
Financial Management System (FMS)
General Security Awareness Training

V 2.1 Updated: September 13, 2006






START HERE GO FURTHER FEDERAL STUDENT AID

Agenda

- **Purpose of Training**
- **FMS Security Profile**
- **User Security Responsibilities**
  - Rules of Behavior
  - Password Management
  - User Contact Information
  - Information Protection
  - System Access Controls
  - Incident Reporting
- **Computer Security Threats**
  - Malicious Software/Programs
  - Social Engineering
  - Theft of Data and/or Equipment
- **Review**
- **Training Acknowledgement**

START HERE GO FURTHER FEDERAL STUDENT AID

Purpose of Training

- Raise the security awareness level of FMS users
- Inform FMS users of information security responsibilities
- Inform users of FMS policies
- Educate users on basic data protection and system security
- This training satisfies the annual requirement for FMS Information Security Training, however your employer or agency may require completion additional training on a periodic basis.

START HERE GO FURTHER FEDERAL STUDENT AID

FMS Security Profile

- FMS is considered to be a Mission Critical system by Federal Student Aid
- FMS Data Sensitivity Ratings
  - Confidentially = MODERATE
  - Integrity = MODERATE
  - Availability = HIGH

- FMS contains data protected under the Privacy Act.
- FMS undergoes system certification and accreditation at least every three years, or after a major system change
- FMS user security awareness training is required annually for all users.

START HERE GO FURTHER FEDERAL STUDENT AID

User Responsibilities

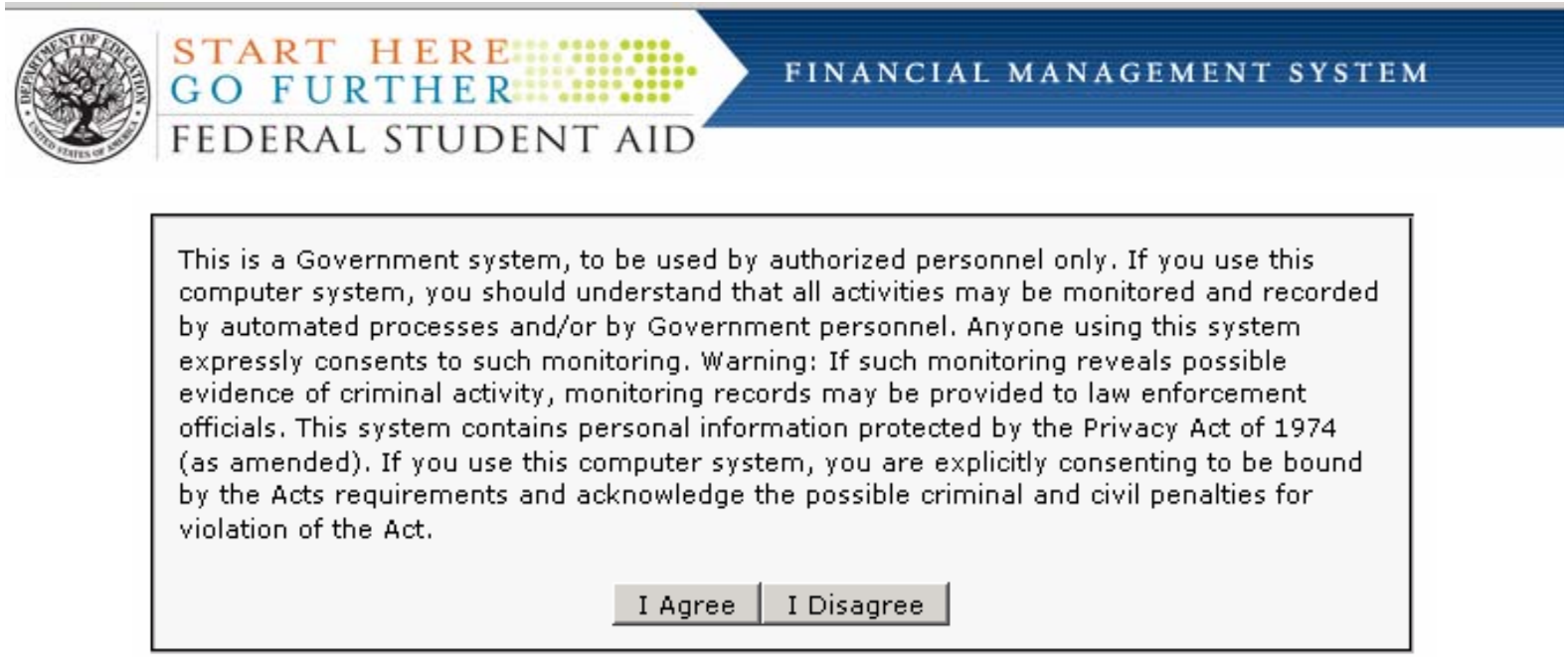
Rules of Behavior

- Prior to being granted access to FMS, all users must read the Rules of Behavior, and submit a signed Security Access Agreement.
- Every user must be made aware of their responsibilities for the use, protection, and release of sensitive Department of Education information under their control. This applies to outsourced support and contractors, as well as government employees.
- Each new user is a risk to the system and to other users of that system. Therefore, everyone must be versed in the rules of the system, or acceptable behavior, before being permitted to access the system. Training is tailored to the needs of the user and the system security requirements.
- Effective security is a team effort involving the participation and support of everyone. It is the responsibility of each user to know and follow these guidelines.
- All new users requesting FMS access MUST receive and maintain a favorable result to a documented background investigation completed by their organization or agency.
- The External User Form contained in the FMS access package highlights the Rules of Behavior that apply when accessing FMS.

User Responsibilities

There should be no expectation of privacy

Users must consent to monitoring with each login to FMS



START HERE GO FURTHER FEDERAL STUDENT AID

User Responsibilities

Password Management

- First time passwords must be used within 30 days or they are inactivated. Contact the FMS help desk for reactivation assistance.
- FMS passwords must be changed every 90 days
- Users who have forgotten their passwords, or experience locked accounts must contact the FMS help desk for assistance.
- FMS passwords must comply with the following requirements
  - Must be at least 8 characters
  - Must be a mix of letters, numbers and symbols or special characters
    - ✓ Upper case letters (A-Z) or Lowercase letters (a – z)
    - ✓ Numerals (0-9)
    - ✓ Special Characters (!,@,#,$,&,*)
  - Must not contain repeating characters (aaa, eee, rrr, @@)

User Responsibilities

Create a Strong Password

- A strong password should appear as a string of random characters.
- Add complexity by combining letters, numbers, and symbols or characters. The greater variety of characters that you have in your password, the harder it is to guess. Use a mix of upper and lower case letters.
- Use words and phrases that are easy for you to remember, but difficult for others to guess.
- Passwords cannot be the same as the username, and cannot contain the word “password” in any form.

START HERE GO FURTHER FEDERAL STUDENT AID

User Responsibilities

Use the following concepts to create a password that is easily remembered, but difficult to guess. Your actual FMS password must be at least 8 characters in length.

- Change letters to numbers and symbols in a string of several words to create a “pass phrase” (i.e., N0MOreCH&NGES).
- Exchange certain letters in a word with a number and symbol, instead of a letter (i.e., HomeRun would become H@M3Run by using the symbol @ for the letter ‘O’ and the number 3 for the letter ‘E’).
- Insert punctuation, numbers and symbols or special characters into a word, and deliberately misspell the word to comply with the “no repeating character” requirement (i.e. 1P@YReiz!).
- Combine a number of personal facts to create a “pass phrase” (i.e., JulyYellowBASEBALL@ 31797SKI).
- Create an acronym from words in a song, a poem, or another known sequence of words (i.e., 4_S&7yA! from the Gettysburg address, “Four score and seven years ago…”).

START HERE GO FURTHER FEDERAL STUDENT AID

User Responsibilities

Keep Your Password Secret !

- Do not share your password. The owner of the password could be held criminally liable for any illegal acts performed using his/her userid & password.
- Your password is the key you use to access FMS information – Protect it!
- For detailed information regarding creating strong passwords, you may wish to visit : http://www.microsoft.com/athome/security/privacy/password.mspx
- Never provide your password over the telephone, via e-mail or based on an e-mail requesting this information.

START HERE GO FURTHER FEDERAL STUDENT AID

User Responsibilities

User Contact Information

- Keep your contact information and email address current.
- The email address on your FMS user access agreement will be used to notify you of FMS security changes, when your access will expire, and when renewals are due.
- Report any change in your email address to the FMS Help Desk.

User Responsibilities

Information Protection

- Mark output, including electronic and hard-copy reports, with the appropriate security classification for Sensitive, Proprietary, or Privacy Act data.
- Distribute information only to authorized personnel.
- Destroy electronic and/or hard-copy material, when discarded (degauss or shred).
- “Clear Desk Policy” - Lock your computer desktop and secure all sensitive data before leaving your desk or workspace.
- Zip and password protect sensitive, proprietary, or Privacy Act data before sending via email.
- Employees and contractors must take all possible security precautions to secure and protect personal privacy information.

User Responsibilities

Information Protection

Output / Media Markings

- **Sensitive** (Caution–Information of National Interest Involved)
- **Privacy Act** (Warning – Privacy Act Information Involved)
  This marking is used to identify information that must be protected under the Privacy Act of 1974 (as amended).
- **PROPIN** (Caution - Proprietary Information Involved)
  This marking is used to identify information provided by a commercial firm or private source under an understanding that the information will be protected.

User Responsibilities

System Access Controls

- Users are permitted access to the system based on their role (role-based-access).
- Application users are restricted from accessing the operating system, other applications, and system resources not needed in the performance of their duties
- Demonstration / training users are not permitted access to live production environments
- Federal Software Usage:
  - No software should be used to gain unauthorized access to the network or scan the network.
  - Do not copy federally owned and provided software for personal use
- E-Mail
  - Do not send unencrypted sensitive information via e-mail
  - ed.gov e-mail addresses are for official FMS related e-mail correspondence only, and are not to be used to create or forward chain letters or “spam” mail.

START HERE GO FURTHER FEDERAL STUDENT AID

User Responsibilities

Incident Reporting

- Report security problems and suspicious activity or incidents
- "Incidents" include, but are not limited to:
  - Data and Equipment Theft and Loss
  - Fraud and Scams
  - System and Data Misuse
  - Phishing, Pharming, Vishing
  - Viruses and Malware
- Report suspected attacks, viruses, password compromise, or rules-of-behavior violations immediately.
- Attempts to exploit a known or suspected flaw in the application or security systems are viewed as malicious activity, and can be considered a crime.
- In the event that you lose privacy-protected personal information, contact your immediate supervisor and your computer security officer immediately. This type of incident must be reported within one-hour under new federal guidelines.

User Responsibilities

Incident Reporting Procedure

- Immediately report incidents to the System Security Officer (SSO):

- FMS SSO:
  - Pamela Jefferson
  - Telephone - 202-377-3491
  - Email: Pamela.Jefferson@ed.gov

- Alternate FMS SSO:
  - Danny Dy Tang
  - Telephone: 202-377-3431
  - Email: Daniel.DyTang@ed.gov

User Responsibilities

Incident Reporting Procedure (cont'd)

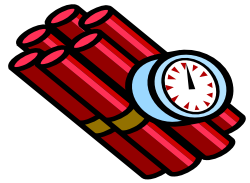
- If ths SSO is not available, report incidents to Federal Student Aid Computer Security Officer (CSO) then contact the FMS SSO as soon as possible:

  Federal Student Aid CSO
  Robert (Bob) Ingwalson
  Telephone: 202-377-3563
  Email : Robert.Ingwalson@ed.gov

- Request email "read receipt" to document receipt of incident report regardless of to whom the incident is reported.

- DO NOT put sensitive details regarding security incidents or vulnerabilities in email or send in documents that are unencrypted. This, in itself, could pose a security risk and incident.

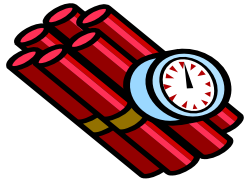
Threats



System Security Threats

- Malicious Software/Programs
  - Malware (viruses, worms) - parasitic programs written intentionally to “infect” or damage program and system performance.
  - Spyware - programs designed to intercept or take partial control of a computer’s operation without the consent of the machine’s owner.
- Social Engineering - an act of deceiving unsuspecting people into revealing confidential information. Includes:
  - Phishing - attempting to fraudulently acquire sensitive information, such as PINs, social security numbers, account numbers, passwords or credit card information, by pretending to be the person or business with whom the victim does business.

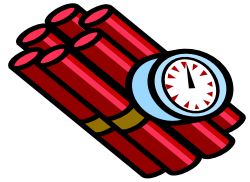
Threats



- Social Engineering (cont'd)
  - Vishing - or "voice phishing" occurs when a scammer sends an email hoping that a victim will telephone a voice mailbox to disclose sensitive financial and personal information.
  - Pharming – An attack aiming to redirect a website's traffic to another (bogus) website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. This is an insidious attack, and not easily detected.
  - Shoulder Surfing - looking over someone's shoulder to get information.

- Theft of Data and/or Equipment

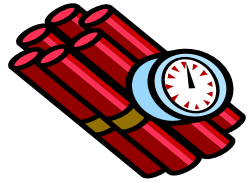
Threats



Protection Against Threats

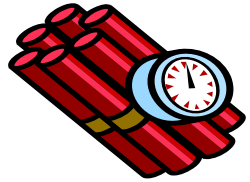
- Malicious Software/Programs: Keep Antivirus and Anti-Spyware Software installed and up-to-date. Don't visit questionable websites, don't click on links sent in email unless from a trusted source, (and even then be wary) report excessively slow computer, or unintended links and images popping up on your screen.
- Social Engineering:
  - Never give out personally identifiable information in an e-mail or to a web site that has a link in an e-mail without validating it with the legitimate source.
  - Never give out your password or PIN to anyone.
  - Do not open email with attachments or enclosures if they are from unknown sources. Do not reply to the e-mail, and Do not type or paste any information into the e-mail.
  - Do not click on any links contained within the e-mail from any unknown source.
  - Use a web-browser tool bar (from a trusted commercial source) that validates the source of the website (Google toolbar is only one such example).
  - Get more information at: http://www.ftc.gov

Threats



Pharming-

- Use anti-virus software, and consider installing a web browser toolbar, anti-spyware, and firewall software (all from trusted, legitimate sources).
- Ensure that your web-browser is kept up to date and security patches are applied.
- Look for website privacy policies. Avoid doing business with any site that does not post its privacy policy.



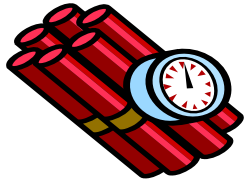
Protection Against Threats

Pharming-cont'd

- Limit the number of websites and amount of personal information you share on the Internet.
- Look for misspelled words and bad formatting.
- If a password is needed, enter an incorrect password first and see what happens.
- Use only a reputable Internet Service Provider.

- Theft of Data and/or Equipment: Secure all equipment and data storage media. Lock screen/terminal when not in use or unattended. Encrypt and guard sensitive data in transit (email / FTP) and at rest (storage).

Threats



Remember!

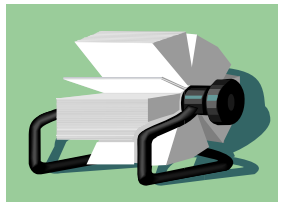
- The Department of Education DOES NOT solicit Privacy Act protected information through emails, nor direct you to web sites through emails that then solicit Privacy Act protected information.

- No one at the Department of Education, including the FMS help desk, will ever ask you for your password. Never disclose your password or PIN to anyone.

- FMS users who receive e-mail requests from unknown sources for sensitive student data should immediately report such incidents to the FMS System Security Officer (SSO).

START HERE GO FURTHER FEDERAL STUDENT AID

Contact Information



FMS Security Points of Contact Review

FMS Help Desk contact information

- 202-377-3888 or 1-800-433-7327

FMS System Security Officers

- Pamela Jefferson, FMS SSO
  Phone: 202-377-3457
  E-mail: Pamela.Jefferson@ed.gov

- Danny DyTang, Alternate FMS SSO
  Phone: 202-377-3431
  E-Mail: Daniel.DyTang@ed.gov

Review

- Report Suspected Incidents and Threats

  If you suspect that your FMS password, or FMS data has been stolen or compromised, contact the FMS SSO immediately.

- Abide by Rules of Behavior
- Observe User Responsibilities
- Protect Sensitive and Privacy Act Data
- Beware of Threats
- Renew your FMS Access Annually!

START HERE GO FURTHER FEDERAL STUDENT AID

Acknowledgement of Training

FMS access will not be granted or renewed until a completed and signed training acknowledgement form is received after the completion of training.

Please fill in the blanks with your name and the date you reviewed the training presentation. Then, fax the completed form or cut-and-paste the following information into an e-mail:

I, _____, hereby certify that I have received, reviewed, and understand the General Information Security Awareness Training for FMS, based on the standards set forth in NIST Special Publication 800-16, as presented. This training is mandatory and fulfills the requirement set forth in OMB Circular A-130, Appendix III. The individual named above received this training on _____, 20___.

_____ _____

*Signature Date

*If sending via e-mail from your registered e-mail account, FMS will consider you to have"signed" this form electronically.

Submit completed form via email to: Ada.Ruth.McIntyre@ed.gov
or via fax to 202-275-3477, Attention: FMS Help Desk